Vereinbarung zur Auftragsverarbeitung

als Anlage zum Dienstleistungsvertrag captis vom 27.06.2023
- nachfolgend „Leistungsvereinbarung“ -

zwischen den Verantwortlichen

Musterschule
Musterstr. 9
99999 Musterstadt
(nachfolgend „Verantwortlicher“ genannt)

und

lambda9 GmbH
Lise-Meitner-Str. 2
24941 Flensburg
(nachfolgend „Auftragsverarbeiter“ genannt)

- beide nachfolgend gemeinsam „Vertragsparteien“ -

wird die folgende Vereinbarung zur Auftragsverarbeitung geschlossen:

Präambel

Die Vertragsparteien sind mit der Leistungsvereinbarung ein Auftragsverarbeitungsverhältnis eingegangen. Um die sich hieraus ergebenden Rechte und Pflichten gemäß den Vorgaben der europäischen Datenschutz-Grundverordnung (Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG - DSGVO), und des Bundesdatenschutzgesetzes (BDSG) zu konkretisieren, schließen die Vertragsparteien die nachfolgende Vereinbarung.

§ 1 Anwendungsbereich

Die Vereinbarung findet Anwendung auf die Erhebung, Verarbeitung und Löschung (im Folgenden: Verarbeitung) aller personenbezogener Daten (im Folgenden: Daten), die Gegenstand der Leistungsvereinbarung sind oder im Rahmen von deren Durchführung anfallen der dem Auftragsverarbeiter bekannt werden.

§ 2 Konkretisierung des Auftragsinhalts

(1) Gegenstand und Dauer der Auftragsverarbeitung sowie Umfang, Art und Zweck der vorgesehenen Verarbeitung von Daten bestimmen sich nach der Leistungsvereinbarung.

(2) Die Art der verarbeiteten Daten ist von der Nutzung durch den Verantwortlichen abhängig. Grundsätzlich werden jegliche Daten verschlüsselt gespeichert, egal welcher Art, um so Sorge dafür zu tragen, dass keinerlei Daten missbräuchlich verwendet werden können.

(3) Das gleiche gilt für den Kreis der durch den Umgang mit ihren Daten betroffenen Personen. Wer Daten zur Verfügung stellt, ist abhängig vom Nutzungsverhalten und dem Einsatzgebiet.

§ 3 Verantwortlichkeit und Weisungsbefugnis

(1) Die Vertragsparteien sind für die Einhaltung der datenschutzrechtlichen Bestimmungen verantwortlich. Der Verantwortliche kann jederzeit die Herausgabe, Berichtigung, Anpassung, Löschung und Einschränkung der Verarbeitung der Daten verlangen.

(2) Zur Gewährleistung des Schutzes der Rechte der betroffenen Personen unterstützt der Auftragsverarbeiter den Verantwortlichen angemessen, insbesondere durch die Gewährleistung geeigneter technischer und organisatorischer Maßnahmen.

(3) Soweit sich eine betroffene Person zwecks Geltendmachung eines Betroffenenrechts unmittelbar an den Auftragsverarbeiter wendet, wird der Auftragsverarbeiter dieses Ersuchen unverzüglich an den Verantwortlichen weiterleiten.

(4) Der Auftragsverarbeiter darf Daten ausschließlich im Rahmen der Weisungen des Verantwortlichen verarbeiten, sofern er nicht zu einer anderen Verarbeitung durch das Recht der Union oder des Mitgliedstaates, dem der Auftragsverarbeiter unterliegt, hierzu verpflichtet ist (z. B. Ermittlungen von Strafverfolgungs- oder Staatsschutzbehörden); in einem solchen Fall teilt der Auftragsverarbeiter dem Verantwortlichen diese rechtlichen Anforderungen vor der Verarbeitung mit, sofern das betreffende Recht eine solche Mitteilung nicht wegen eines wichtigen öffentlichen Interesses verbietet (Art. 28 Abs. 3 Satz 2 lit. a DSGVO). Eine Weisung ist die auf einen bestimmten Umgang des Auftragsverarbeiters mit Daten gerichtete schriftliche, elektronische oder mündliche Anordnung des Verantwortlichen. Die Anordnungen sind zu dokumentieren. Die Weisungen werden zunächst durch die Leistungsvereinbarung definiert und können von dem Verantwortlichen danach in dokumentierter Form durch eine einzelne Weisung geändert, ergänzt oder ersetzt werden.

(5) Der Auftragsverarbeiter hat den Verantwortlichen unverzüglich zu informieren, wenn er der Meinung ist, eine Weisung verstoße gegen datenschutzrechtliche Vorschriften. Der Auftragsverarbeiter ist berechtigt, die Durchführung der entsprechenden Weisung solange auszusetzen, bis sie von Seiten des Verantwortlichen bestätigt oder geändert wird.

(6) Änderungen des Verarbeitungsgegenstandes mit Verfahrensänderungen sind gemeinsam abzustimmen und zu dokumentieren. Auskünfte an Dritte oder die betroffene Person darf der Auftragsverarbeiter nur nach vorheriger ausdrücklicher schriftlicher Zustimmung durch den Verantwortlichen erteilen. Der

Auftragsverarbeiter verwendet die Daten für keine anderen Zwecke und ist insbesondere nicht berechtigt, sie an Dritte weiterzugeben. Kopien und Duplikate werden ohne Wissen des Verantwortlichen nicht erstellt.

(7) Der Verantwortliche führt das Verzeichnis von Verarbeitungstätigkeiten i.S.d. Art. 30 Abs. 1 DSGVO. Der Auftragsverarbeiter stellt dem Verantwortlichen auf dessen Wunsch Informationen zur Aufnahme in das Verzeichnis zur Verfügung. Der Auftragsverarbeiter führt entsprechend den Vorgaben des Art. 30 Abs. 2 DSGVO ein Verzeichnis zu allen Kategorien von im Auftrag des Verantwortlichen durchgeführten Tätigkeiten der Verarbeitung.

(8) Die Verarbeitung der Daten im Auftrag des Verantwortlichen findet ausschließlich auf dem Gebiet der Europäischen Union und damit im Geltungsbereich der DSGVO statt. Eine Verarbeitung in einem Staat außerhalb des in Satz 1 genannten Territoriums ist nur zulässig, wenn sichergestellt ist, dass unter Berücksichtigung der Voraussetzungen des Kapitels V der DSGVO das durch die DSGVO gewährleistete Schutzniveau nicht unterlaufen wird und bedarf der vorherigen ausdrücklichen schriftlichen Zustimmung des Verantwortlichen. Die grundlegenden Voraussetzungen für die Rechtmäßigkeit der Verarbeitung bleiben unberührt.

(9) Der Auftragsverarbeiter stellt sicher, dass ihm unterstellte natürliche Personen, die Zugang zu Daten haben, diese nur auf Anweisung des Verantwortlichen verarbeiten. Eine Verarbeitung von Daten außerhalb der Betriebsräume des Auftragsverarbeiters (z.B. Telearbeit, Heimarbeit, Home Office, mobiles Arbeiten) bedarf der vorherigen ausdrücklichen schriftlichen Zustimmung des Verantwortlichen, die erst nach Festlegung angemessener technischer und organisatorischer Maßnahmen für die Verarbeitungssituation erteilt werden kann.

§ 4 Beachtung zwingender gesetzlicher Pflichten durch den Auftragsverarbeiter

(1) Der Auftragsverarbeiter stellt sicher, dass sich die zur Verarbeitung der Daten befugten Personen zur Vertraulichkeit verpflichtet haben oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen und weist dies dem Verantwortlichen auf Wunsch nach. Dies umfasst auch die Belehrung über die in diesem Auftragsverarbeitungsverhältnis bestehende Weisungs- und Zweckbindung.

(2) Die Vertragsparteien unterstützen sich gegenseitig beim Nachweis und der Dokumentation der ihnen obliegenden Rechenschaftspflicht im Hinblick auf die Grundsätze ordnungsgemäßer Datenverarbeitung, einschließlich der Umsetzung der notwendigen technischen und organisatorischen Maßnahmen (Art. 5 Abs. 2, Art. 24 Abs. 1 DSGVO). Der Auftragsverarbeiter stellt dem Verantwortlichen hierzu bei Bedarf entsprechende Informationen zur Verfügung.

(3) Der Auftragsverarbeiter hat eine/n Datenschutzbeauftragte/n zu benennen, die/der ihre/seine Tätigkeit entsprechend den gesetzlichen Vorschriften ausübt. Die Kontaktdaten der/des Datenschutzbeauftragten sind dem Verantwortlichen zum Zwecke der direkten Kontaktaufnahme mitzuteilen.

(4) Der Auftragsverarbeiter informiert den Verantwortlichen unverzüglich über Kontrollen und Maßnahmen durch die Aufsichtsbehörden oder falls eine Aufsichtsbehörde im Rahmen ihrer Zuständigkeit bei dem Auftragsverarbeiter anfragt, ermittelt oder sonstige Erkundigungen einzieht.

§ 5 Technisch-organisatorische Maßnahmen und deren Kontrolle

(1) Die Vertragsparteien vereinbaren die in dem Anhang „Technisch-organisatorische Maßnahmen“ zu dieser Vereinbarung niedergelegten konkreten technischen und organisatorischen Sicherheitsmaßnahmen. Der Anhang ist Gegenstand dieser Vereinbarung.

(2) Technische und organisatorische Maßnahmen unterliegen dem technischen Fortschritt. Insoweit ist es dem Auftragsverarbeiter gestattet, alternative adäquate Maßnahmen umzusetzen. Dabei darf das Sicherheitsniveau der in dem Anhang „Technisch-organisatorische Maßnahmen“ festgelegten Maßnahmen nicht unterschritten werden. Wesentliche Änderungen sind zu dokumentieren.

(3) Der Auftragsverarbeiter wird dem Verantwortlichen alle erforderlichen Informationen zur Verfügung stellen, die zum Nachweis der Einhaltung der in dieser Vereinbarung getroffenen und der gesetzlichen Vorgaben erforderlich sind. Der Auftragsverarbeiter unterstützt den Verantwortlichen unter Berücksichtigung der Art der Verarbeitung und der ihm zur Verfügung stehenden Informationen in angemessener Art und Weise bei der Einhaltung der in den Art. 32 bis 36 DSGVO genannten Pflichten. Er wird insbesondere Überprüfungen/Inspektionen, die vom Verantwortlichen oder einem anderen von diesem beauftragten

Prüfer durchgeführt werden, ermöglichen und deren Durchführung unterstützen. Der Nachweis der Umsetzung solcher Maßnahmen, die nicht nur den konkreten Auftrag betreffen, kann dabei auch durch Vorlage eines aktuellen Testats, von Berichten hinreichend qualifizierter und unabhängiger Instanzen (z.B. Wirtschaftsprüfer, unabhängige Datenschutzauditoren), durch die Einhaltung genehmigter Verhaltensregeln nach Art. 40 DSGVO, einer Zertifizierung nach Art. 42 DSGVO oder einer geeigneten Zertifizierung durch IT-Sicherheits- oder Datenschutzaudit (z.B. nach BSI-Grundschutz) erbracht werden. Der Auftragsverarbeiter verpflichtet sich, den Verantwortlichen über den Ausschluss von genehmigten Verhaltensregeln gemäß Art. 41 Abs. 4 DSGVO, den Widerruf einer Zertifizierung gemäß Art. 42 Abs. 7 und jede andere Form der Aufhebung oder wesentlichen Änderung der vorgenannten Nachweise unverzüglich zu unterrichten.

(4) Der Verantwortliche kann sich jederzeit zu Prüfzwecken in den Betriebsstätten des Auftragsverarbeiters zu den üblichen Geschäftszeiten ohne Störung des Betriebsablaufs von der Angemessenheit der Maßnahmen zur Einhaltung der gesetzlichen Vorgaben oder der zur Durchführung dieses Vertrages erforderlichen technischen und organisatorischen Erfordernisse überzeugen.

(5) Der Auftragsverarbeiter stellt dem Verantwortlichen darüber hinaus alle erforderlichen Informationen zur Verfügung, die er für die Prüfungen nach Absatz 4 sowie für eine Abschätzung der Folgen der vorgesehenen Verarbeitungsvorgänge für den Schutz der Daten (Datenschutz- Folgenabschätzung i.S.d. Art. 35 DSGVO) benötigt.

(6) Der Auftragsverarbeiter hat im Benehmen mit dem Verantwortlichen alle erforderlichen Maßnahmen zur Sicherung der Daten bzw. der Sicherheit der Verarbeitung, insbesondere auch unter Berücksichtigung des Stands der Technik, sowie zur Minderung möglicher nachteiliger Folgen für Betroffene zu ergreifen.

§ 6 Mitteilung bei Verstößen durch den Auftragsverarbeiter

Der Auftragsverarbeiter unterrichtet den Verantwortlichen unverzüglich bei schwerwiegenden Störungen seines Betriebsablaufes, bei Verdacht auf Verstöße gegen diese Vereinbarung sowie gesetzliche Datenschutzbestimmungen, bei Verstößen gegen solche Bestimmungen oder anderen Unregelmäßigkeiten bei der Verarbeitung der Daten des Verantwortlichen. Dies gilt insbesondere im Hinblick auf die Meldepflicht nach Art. 33 Abs. 2 DSGVO sowie auf korrespondierende Pflichten des Verantwortlichen nach Art. 33 und Art. 34 DSGVO. Der Auftragsverarbeiter sichert zu, den Verantwortlichen erforderlichenfalls bei seinen Pflichten nach Art. 33 und 34 DSGVO angemessen zu unterstützen. Meldungen nach Art. 33 oder 34 DSGVO für den Verantwortlichen darf der Auftragsverarbeiter nur nach vorheriger Weisung gem. § 3 dieses Vertrages durchführen.

§ 7 Löschung und Rückgabe von Daten

(1) Überlassene Datenträger und Datensätze verbleiben im Eigentum des Verantwortlichen.

(2) Nach Abschluss der vertraglich vereinbarten Leistungen oder früher nach Aufforderung durch den Verantwortlichen, jedoch spätestens mit Beendigung der Leistungsvereinbarung, hat der Auftragsverarbeiter sämtliche in seinen Besitz gelangte Unterlagen, erstellte Verarbeitungs- und Nutzungsergebnisse sowie Datenbestände (wie auch hiervon gefertigte Kopien oder Reproduktionen), die im Zusammenhang mit dem Auftragsverhältnis stehen, dem Verantwortlichen auszuhändigen oder nach vorheriger Zustimmung des Verantwortlichen datenschutzgerecht zu vernichten. Hierbei besteht für den Verantwortlichen das Wahlrecht zur Aushändigung oder Vernichtung, macht der Verantwortliche von diesem Wahlrecht keinen Gebrauch, gilt die Vernichtung als vereinbart. Gleiches gilt für Test- und Ausschussmaterial. Ein Löschungsprotokoll ist dem Verantwortlichen auf Anforderung vorzulegen.

(3) Der Auftragsverarbeiter kann Dokumentationen, die dem Nachweis der auftrags- und ordnungsgemäßen Datenverarbeitung dienen, entsprechend der jeweiligen Aufbewahrungsfristen bis zu deren Ende auch über das Vertragsende hinaus aufbewahren. Alternativ kann er sie zu seiner Entlastung bei Vertragsende dem Verantwortlichen übergeben. Für die nach Satz 1 aufbewahrten Daten gelten nach Ende der Aufbewahrungsfrist die Pflichten nach Absatz 2.

§ 8 Subunternehmen

(1) Die zur Erfüllung dieses Vertrages hinzugezogenen Subunternehmen sind in der Anlage Subunternehmer im Einzelnen bezeichnet. Mit deren Beauftragung erklärt sich der Verantwortliche einverstanden. Der Auftragsverarbeiter darf weitere Auftragsverarbeiter (Subunternehmen) nur mit vorheriger ausdrücklicher schriftlicher Zustimmung des Verantwortlichen in Anspruch nehmen. Sofern es sich um eine allgemeine

schriftliche Genehmigung handelt, informiert der Auftragsverarbeiter den Verantwortlichen unverzüglich über jede beabsichtigte Änderung in Bezug auf die Hinzuziehung oder die Ersetzung von Subunternehmen. Der Verantwortliche kann gegen derartige Änderungen Einspruch erheben. Nicht als Leistungen von Subunternehmen im Sinne dieser Regelung gelten Dienstleistungen, die der Auftragsverarbeiter bei Dritten als Nebenleistung zur Unterstützung der Auftragsdurchführung in Anspruch nimmt, beispielsweise Telekommunikationsdienstleistungen. Der Auftragsverarbeiter ist jedoch verpflichtet, zur Gewährleistung des Schutzes und der Sicherheit der Daten des Verantwortlichen auch bei fremd vergebenen Nebenleistungen angemessene und gesetzeskonforme vertragliche Vereinbarungen zu treffen sowie Kontrollmaßnahmen zu ergreifen.

(2) Wenn Subunternehmen durch den Auftragsverarbeiter eingeschaltet werden, hat der Auftragsverarbeiter sicherzustellen, dass seine vertraglichen Vereinbarungen mit dem Subunternehmen so gestaltet sind, dass das Datenschutzniveau mindestens der Vereinbarung zwischen dem Verantwortlichen und dem Auftragsverarbeiter entspricht und alle vertraglichen und gesetzlichen Vorgaben beachtet werden; dies gilt insbesondere auch im Hinblick auf den Einsatz geeigneter technischer und organisatorischer Maßnahmen zur Gewährleistung eines angemessenen Sicherheitsniveaus der Verarbeitung.

(3) Dem Verantwortlichen sind in der vertraglichen Vereinbarung mit dem Subunternehmen Kontroll- und Überprüfungsrechte entsprechend dieser Vereinbarung einzuräumen. Ebenso ist der Verantwortlichen berechtigt, auf schriftliche Anforderung vom Auftragsverarbeiter Auskunft über den Inhalt des mit dem Subunternehmen geschlossenen Vertrages und die darin enthaltene Umsetzung der datenschutzrelevanten Verpflichtungen des Subunternehmens zu erhalten.

(4) Kommt das Subunternehmen seinen datenschutzrechtlichen Verpflichtungen nicht nach, so haftet der Auftragsverarbeiter gegenüber dem Verantwortlichen für die Einhaltung der Pflichten des Subunternehmens. Der Auftragsverarbeiter hat in diesem Falle auf Verlangen des Verantwortlichen die Beschäftigung des Subunternehmens ganz oder teilweise zu beenden oder das Vertragsverhältnis mit dem Subunternehmen zu lösen, wenn und soweit dies nicht unverhältnismäßig ist.

§ 9 Datenschutzkontrolle

Der Auftragsverarbeiter verpflichtet sich, der/dem Datenschutzbeauftragten des Verantwortlichen sowie der zuständigen Aufsichtsbehörde zur Erfüllung ihrer jeweiligen gesetzlichen zugewiesenen Aufgaben im Zusammenhang mit diesem Auftrag jederzeit Zugang zu den üblichen Geschäftszeiten zu gewähren. Der Auftragsverarbeiter unterwirft sich zusätzlich zu der für ihn bestehenden gesetzlichen Datenschutzaufsicht der Kontrolle der für den Verantwortlichen bestehenden Datenschutzaufsicht und der Kontrolle durch die/den Datenschutzbeauftragten des Verantwortlichen mit Ausnahme der Bereiche, die keinerlei Bezug zur Auftragserfüllung haben. Er duldet insbesondere Betretungs-, Einsichts- und Fragerechte der Genannten einschließlich der Einsicht in durch Berufsgeheimnisse geschützte Unterlagen. Er wird seine Mitarbeiter anweisen, mit den Genannten zu kooperieren, insbesondere deren Fragen wahrheitsgemäß und vollständig zu beantworten. Die nach Gesetz bestehenden Verschwiegenheitspflichten und Zeugnisverweigerungsrechte der Genannten bleiben davon unberührt.

§ 10 Schlussbestimmungen

(1) Änderungen und Ergänzungen dieser Anlage und aller ihrer Bestandteile - einschließlich etwaiger Zusicherungen des Auftragsverarbeiters - bedürfen einer schriftlichen Vereinbarung und des ausdrücklichen Hinweises darauf, dass es sich um eine Änderung bzw. Ergänzung dieser Bedingungen handelt. Dies gilt auch für den Verzicht auf dieses Formerfordernis.

(2) Sollten einzelne Regelungen dieser Vereinbarung unwirksam oder undurchführbar sein, wird davon die Wirksamkeit der übrigen Regelungen nicht berührt. An die Stelle der unwirksamen oder undurchführbaren Regelung tritt diejenige wirksame und durchführbare Regelung, deren Wirkungen der Zielsetzung am nächsten kommt, die die Vertragsparteien mit der unwirksamen oder undurchführbaren Bestimmung verfolgt haben. Die vorstehenden Bestimmungen gelten entsprechend für den Fall, dass sich die Vereinbarung als lückenhaft erweist.

Anhang „Technisch-organisatorische Maßnahmen“

zur Vereinbarung zur Auftragsverarbeitung vom 27.06.2023 zwischen

Musterschule
Musterstr. 9
99999 Musterstadt
(nachfolgend „Verantwortlicher“ genannt)

und

lambda9 GmbH
Lise-Meitner-Str. 2
24941 Flensburg
(nachfolgend „Auftragsverarbeiter“ genannt)

§5 der Vereinbarung zur Auftragsverarbeitung verweist zur Konkretisierung der technisch- organisatorischen Maßnahmen auf diesen Anhang.

§ 1 Technische und organisatorische Sicherheitsmaßnahmen

Die Vertragspartner sind verpflichtet, geeignete technische und organisatorische Maßnahmen so durchzuführen, dass die Verarbeitung der Daten im Einklang mit den gesetzlichen Anforderungen erfolgt und der Schutz der Rechte der betroffenen Person in angemessener Form gewährleistet ist.

§ 2 Innerbetriebliche Organisation des Auftragsverarbeiters

Der Auftragsverarbeiter wird seine innerbetriebliche Organisation so gestalten, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird. Dabei sind insbesondere Maßnahmen zu treffen, die je nach der Art der zu schützenden Daten oder Datenkategorien geeignet sind.

§ 3 Konkretisierung der Einzelmaßnahmen

(1) Im Einzelnen werden folgende Maßnahmen bestimmt, die der Umsetzung der Vorgaben des Art. 32 DSGVO dienen:

Nr.	Maßnahme	Umsetzung der Maßnahme
Pseudonymisierung (Art. 32 Abs. 1 lit. a) DSGVO) Sofern ein Kunde personenbezogene Daten im Auftrag der lambda9 GmbH verarbeiten lässt und Wert auf eine Pseudonymisierung oder Anonymisierung, werden entsprechende Techniken implementiert.		
Vertraulichkeit (Art. 32 Abs. 1 lit. b) DSGVO)		
1.	**Verschlüsselung**	Alle Daten, die die lamda 9 GmbH verarbeitet werden im Ruhezustand ausschließlich verschlüsselt gespeichert.
2.	**Zutrittskontrolle** Unbefugten ist der Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet werden, zu verwehren.	Die Geschäftsräume des Auftragsverarbeiter sind durch elektronische Schlösser („Transponder“) gegen unbefugtes Betreten gesichert und außerhalb der Geschäftszeiten bzw. bei nicht-Anwesenheit stets verschlossen. Transponder werden ausschließlich an Mitarbeiter ausgegeben und müssen vor Austritt aus dem Unternehmen wieder zurückgegeben werden.

3.	**Zugangskontrolle** Es ist zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können.	Generell werden Zugangsberechtigungen zu relevanten Anwendungen oder Systemen nur bestimmbaren Personen (persönliche Logins) zugeordnet. Die Erteilung der Zugangsberechtigung erfolgt nur nach einem definierten und dokumentierten Prozess. Erteilte Zugangsberechtigungen werden entsprechend des definierten Prozesses dokumentiert. Sobald ein Zugang nicht mehr erforderlich ist, wird die Zugangsberechtigung wieder entzogen. Der Entzug einer Zugangsberechtigung erfolgt nach einem definierten und dokumentierten Prozess. Alle Arbeitsplatzrechner/Laptops sind vollständig verschlüsselt und die darauf gespeicherten Daten somit auch nach Diebstahl für Dritte nicht einsehbar. Der Zugang zu Daten in IT-Systemen wird immer auf den notwendigen Personenkreis eingeschränkt. Der Zugang wird mittels technischer Verfahren wie • Passwort • Zertifikaten • Public Key geschützt. Je nach Anforderung und System wird das sicherste Verfahren gewählt.
4.	**Zugriffskontrolle** Es ist zu gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können, und dass personenbezogene Daten bei der Verarbeitung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können.	Es ist ein Login jedes Benutzers erforderlich, um Daten auf dem System des Verantwortlichen einsehen bzw. verarbeiten zu können. Der Login wird mit einem Passwort und optional durch eine durch den Benutzer zu aktivierende Zwei-Faktor-Authentifizierung (2FA) auf Basis eines One Time Password (OTP) Generators abgesichert. Das verwendete Passwort muss mindestens einen Groß und einen Kleinbuchstaben enthalten sowie mindestens 10 Zeichen lang sein. Unerlaubte Tätigkeiten in IT-Systemen außerhalb von Berechtigungen sind zu verhindern. Der Zugriff auf personenbezogene Daten wird auf den notwendigen Benutzerkreis eingeschränkt. Der anonyme Zugriff auf personenbezogene Daten wird verhindert.
5.	**Trennungsgebot** Es ist zu gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können. Alle Projekte werden getrennt voneinander bearbeitet.	Sofern Daten für die Bearbeitung erforderlich sind, werden jeweils eigene Datenbankinstanzen je Entwicklungsprojekt betrieben, um eine Vermischung von Daten unterschiedlicher Projekte/Kunden zu vermeiden. Daten, die zu unterschiedlichen Zwecken erhoben wurden, werden getrennt verarbeitet. Auf dedizierten Systemen für einen bestimmten Kunden werden keine Daten eines anderen Kunden eingelesen. Bei zentralen Systemen, in denen Daten mehrerer Kunden verarbeitet werden, werden stets Merkmale mitgeführt, die eine eindeutige Zuordnung zum jeweiligen Kunden gewährleisten. Sollen personenbezogene Daten an eine Stelle außerhalb der lambda9 GmbH übermittelt werden, erfolgt zunächst eine kundengenaue Trennung dieser Daten. Wird ein Test-System mit eigenen personenbezogenen Daten benötigt, so gelten für das Test-System die gleichen Regeln wie für das Produktions-System.
Integrität (Art. 32 Abs. 1 lit. b) DSGVO)		
6.	**Weitergabekontrolle**	Der Auftragsverarbeiter bietet dem Verantwortlichen ausdrücklich jederzeit die Verschlüsselung von E-

	Es ist zu gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können, und dass überprüft und festgestellt werden kann, an welche Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist.	Mails mittels OpenPGP an. Macht der Verantwortliche von keinem dieser Verfahren Gebrauch, verpflichten sich Auftragsverarbeiter sowie Verantwortlicher der jeweils anderen Seite keinerlei personenbezogene oder anderweitig sensible Daten (z.B. Zugänge, Passwörter etc.) per Email zu übermitteln. Die Anwendung selbst stellt ohne explizite Aktivierung durch den Nutzer keine Informationen zu, berechtigte Benutzer sind nur in der Lage nach einem qualifizierten Login die Daten zu entschlüsseln und über eine verschlüsselte Datenverbindung herunterzuladen.
7.	**Eingabekontrolle** Es ist zu gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind.	Die IT-Systeme sind so konstruiert, dass eine Änderung/ Speicherung von Daten nur mit dem Datum/Uhrzeit und der Angabe des Bearbeiters, basierend auf dem eingeloggten Benutzer, in der Datenbank vollzogen werden kann. Es ist jederzeit eine Änderungshistorie des Datenbestandes nachvollziehbar.
Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b) DSGVO) sowie rasche Wiederherstellbarkeit (Art. 32 Abs. 1 lit. c) DSGVO)		
8.	**Verfügbarkeitskontrolle** Es ist zu gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind.	Es werden regelmäßige Backups der Daten durchgeführt, die getrennt von den Quelldaten aufbewahrt werden und ein Zurückholen der Informationen im unwahrscheinlichen Fall des Datenverlustes gewährleisten.
9.	**Rasche Wiederherstellbarkeit**	Für die aus Datenschutzsicht kritischen Prozesse im Unternehmen wurden spezielle Notfallpläne erstellt. Diese beinhalten Informationen zum geplanten Vorgehen in datenschutzrelevanten Notfallsituationen (z.B. Verlust von personenbezogenen Daten). Auch die notwendigen Kommunikationsinhalte, -kanäle und -empfänger werden konkret benannt, um sicherzustellen, dass alle betroffenen Personen zeitnah über den jeweiligen Notfall informiert werden. Welche Prozesse als kritisch einzustufen sind, wurde von dem Datenschutzverantwortlichen im Unternehmen definiert.
Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Art. 32 Abs. 1 lit. d) DSGVO)		
10.	**Datenschutzmanagement**	Die Unternehmensleitung hat die Verantwortung für Datenschutz und Informationssicherheit übernommen und eine entsprechende Leitlinie veröffentlicht. Gleiches gilt für Richtlinien für Beschäftigte zum Umgang mit personenbezogenen Daten. Diese sind Teil des implementierten Datenschutzmanagementsystems (DSMS). Kommunikation von Verhaltensrichtlinien zum Thema Datenschutz an alle Mitarbeiter Bei Eintritt in das Unternehmen werden alle wesentlichen Verhaltensrichtlinien zum Thema Datenschutz in schriftlicher wie persönlicher Form an neue Mitarbeiter kommuniziert. Neben unserem grundsätzlichen Verständnis vom Umgang mit personenbezogenen Daten vermitteln wir auch das notwendige Wissen zur korrekten Anwendung aller technischen und organisatorischen Datenschutzmaßnahmen.

		Regelmäßige Unterweisung und Fortbildung von Mitarbeitern zum Thema Datenschutz Unsere Mitarbeiter werden regelmäßig zu relevanten Datenschutzthemen geschult. Dabei werden sowohl Grundlagen aufgefrischt als auch aktuelle Themen sowie rechtliche Änderungen vermittelt. Neben den entsprechenden datenschutztechnischen Kompetenzen soll so eine hohe Sensibilität für den Schutz personenbezogener Daten bei allen Mitarbeitern gefördert werden. Die Schulungen finden mindestens einmal jährlich statt und werden durch entsprechende Nachweise belegt. Unterzeichnung einer Verpflichtungserklärung zur Wahrung der Vertraulichkeit und zur Wahrung von Betriebs- und Geschäftsgeheimnissen durch alle Mitarbeiter Alle Beschäftigten werden schriftlich zum vertraulichen Umgang mit personenbezogenen Daten und zur Wahrung von Betriebs- und Geschäftsgeheimnissen verpflichtet. Darüber hinaus wird der Mitarbeiter über mögliche Folgen von Verstößen gegen die Verpflichtungserklärung aufgeklärt. Alle in der Verpflichtungserklärung vereinbarten Punkte gelten auch über den Zeitraum der Anstellung hinaus. Die Verpflichtung wird in der Personalabteilung aufbewahrt und durch den Datenschutzbeauftragten auditiert. Durchführung von Audits durch den externen DSB Es erfolgt regelmäßig (mindestens einmal jährlich) ein Audit durch den externen DSB. Dieser erhält Zutritt zum Unternehmen sowie Zugriff auf alle datenschutzrelevanten Informationen und Unterlagen, um sich so ein objektives Bild vom Datenschutzniveau im Unternehmen machen zu können. Sinnvolle Optimierungen werden anschließend gemeinsam mit dem DSB implementiert und an die Mitarbeiter kommuniziert. Jährliche Überprüfung der Wirksamkeit der ergriffenen Schutzmaßnahmen Unabhängig von zusätzlich durchgeführten externen Audits, erfolgt jährlich eine innerbetriebliche Überprüfung zur Wirksamkeit der ergriffenen technischen und organisatorischen Schutzmaßnahmen. Hierzu werden die aktuellen Schutzmaßnahmen gemeinsam mit Vertretern aller Verantwortungsbereiche beleuchtet und sofern sinnvoll entsprechende Optimierungen festgelegt.
11.	**Incident-Response-Management**	Dokumentation von datenschutzrelevanten Zwischenfällen Datenschutzrelevante Zwischenfälle, bei denen nicht ausgeschlossen werden kann, dass personenbezogene Daten gelöscht oder an unberechtigte Dritte weitergeleitet wurden, werden umfassend dokumentiert. Die Unterlagen dienen zum einen einer lückenlosen Kommunikation an die Datenschutzbehörden sowie die betroffenen Kunden, zum anderen können auf Basis dieser Informationen Verbesserungen umgesetzt werden, die ähnliche Vorfälle zukünftig verhindern.

12.	**Datenschutz durch Technikgestaltung und datenschutzfreundliche Voreinstellung**	Bevor eine Soft- oder Hardware angeschafft wird, wird evaluiert, ob das Gebot zur Umsetzung von Datenschutz durch Technikgestaltung und datenschutzfreundliche Voreinstellungen (nach Art. 25 DSGVO) eingehalten werden kann. Hierzu werden die beiden Aspekte vor dem Einsatz der jeweiligen Soft- oder Hardware betrachtet. Es ist ein Verzeichnis von Verarbeitungstätigkeiten i.S.d. Art. 30 Abs. 1 und 2 DSGVO erstellt worden.
13.	**Auftragskontrolle**	Sämtliche Informationen des Verantwortlicher werden nur solche Mitarbeiter des Auftragsverarbeiters zugänglich gemacht, die mit der Leistungserfüllung betraut sind. Bei der Beauftragung von Dienstleistern und Partnern erfolgt vorab ein Vergleich möglicher Anbieter unter Datenschutzaspekten. Hierzu holen wir je nach Art und Umfang des Auftrags Informationen zur Verarbeitung von personenbezogenen Daten beim jeweiligen Anbieter ein. Bewertet werden Aspekte wie die Übermittlung von Daten, deren konkrete Verarbeitung sowie die getroffenen technischen und organisatorischen Schutzmaßnahmen. Eine Zusammenarbeit erfolgt ausschließlich mit Dienstleistern und Partnern, die das geforderte Datenschutzniveau glaubhaft sicherstellen können. Das Auswahlverfahren wird in geeigneter und nachvollziehbarer Form dokumentiert. Das Auftragsverhältnis ist detailliert und schriftlich durch einen Auftragsverarbeitungsvertrag (AVV) geregelt.

Anhang „Subunternehmen“

zur Vereinbarung zur Auftragsverarbeitung vom 27.06.2023 zwischen

Musterschule
Musterstr. 9
99999 Musterstadt
(nachfolgend „Verantwortlicher“ genannt)

und

lambda9 GmbH
Lise-Meitner-Str. 2
24941 Flensburg
(nachfolgend „Auftragsverarbeiter“ genannt)

§ 8 der Vereinbarung zur Auftragsverarbeitung verweist zur Konkretisierung der Subunternehmen auf diesen Anhang.

Folgende Subunternehmen werden vom Auftragsverarbeiter per Dienstleistungsvertrag für unterstützende Leistungen beauftragt:

Nr.	Unternehmen	Einsatzgebiet
1.	**IONOS SE** - Website & eCommerce Platforms, Hinterm Hauptbahnhof 3-5 in 76137 Karlsruhe	Serverbetrieb

Technisch-organisatorische Maßnahmen des Subunternehmens

Das Subunternehmen verpflichtet sich gegenüber dem Auftragsverarbeiter zur Einhaltung der technischen und organisatorischen Maßnahmen, die zur Einhaltung der anzuwendenden Datenschutzvorschriften erforderlich sind. Dies beinhaltet insbesondere die Vorgaben aus Art. 32 DSGVO.

Werden personenbezogene Daten automatisiert verarbeitet oder genutzt, ist die innerbetriebliche Organisation so zu gestalten, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird. Dabei sind insbesondere Maßnahmen zu treffen, die je nach der Art der zu schützenden personenbezogenen Daten oder Datenkategorien geeignet sind. Das Subunternehmen hat insbesondere die folgenden Maßnahmen getroffen. Grundsätzlich ist eine Nutzung der Datenverarbeitungssysteme durch den Rechenzentrumsbetreiber nicht vorgesehen.

1. Unbefugten den Zutritt zu Datenverarbeitungsanlagen, mit denen die personenbezogenen Daten verarbeitet und genutzt werden, zu verwehren **(Zutrittskontrolle)**:

Die Räumlichkeiten des Subunternehmens befinden sich in einem ausschließlich geschäftlich genutzten Haus. Sämtliche Zugänge sind ausreichend gegen den unbefugten Zutritt abgesichert, das bedeutet dass:

• Jedwede Außentüren mit einem manuellen und technischen Schließsystem versehen und grundsätzlich verschlossen sind;
• die den Mitarbeitern zur Verfügung gestellten Schlüssel personengebunden registriert sowie die Schlüsselausgabe quittiert wird;
• Besucher nur in Begleitung eines Mitarbeiters sich in den Räumlichkeiten bewegen können;
• Personal von Dritten, insbesondere für Reinigungs- und Wartungsaufgaben sorgfältig ausgewählt wird.

Im Rahmen des Rechenzentrumsbetriebes wird darauf geachtet, dass:

• der Zutritt zum Rechenzentrum nur autorisierten Personen gestattet ist;
• der Zutritt durch ein materielles (RFID-Chip) und ein geistigen (PIN) Identifikationsmerkmal gesichert ist. Es wird zwischen fest zugewiesenen und beim Sicherheitsdienst zur Abholung hinterlegten Zutrittsberechtigungen unterschieden. Bei Zutrittsberechtigungen, die zur Abholung hinterlegt sind, wird die Autorisierung durch Kontrolle des Personalausweises sichergestellt. Die Daten werden bei einem Sicherheitsdienst hinterlegt (Whitelist), so wird gewährleistet, dass nur berechtigte Personen das Rechenzentrum betreten können;
• der Zutritt zu den einzelnen Kundenschränken oder -flächen ausschließlich durch den Kunden und durch das zuständige Personal möglich ist;
• die Zutrittskontrollsysteme sowie die Alarmanlagen über USV und Netzersatzanlage gegen Stromausfall gesichert sind;
• das Rechenzentrum, insbesondere der Zutritt zu Sicherheitsbereichen mit Videoüberwachung ausgestattet ist;
• das Rechenzentrum regelmäßig innerhalb vorgegebener Zeitfenster durch einen Wachdienst begangen wird. Die zu überprüfenden Punkte, welche der Wachdienst in den Rechenzentren zu kontrollieren hat, sind festgelegt. Auffälligkeiten werden berichtet.

2. Zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können **(Zugangskontrolle)**:

Es erfolgt insbesondere eine authentifizierte Benutzeridentifikation, insbesondere dadurch, dass:

• alle technischen Systeme (zentral und dezentral), Hardware und Software Firewall geschützt sind;
• der vorhandene Virenschutz (Anti-Virensoftware) gepflegt und aktualisiert wird;
• der Zugang zu Serverräumen nur einer begrenzten Anzahl von Personen gestattet wird (restricted area);
• Mitarbeiter ausschließlich mit den personalisiert angelegten Benutzerprofilen arbeiten.
• VPN-Technologie (SSL/TLS) eingesetzt wird;

3. Dafür Sorge zu tragen, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können, und dass personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können **(Zugriffskontrolle)**:

Die unerlaubte Tätigkeit in Datenverarbeitungssystemen außerhalb eingeräumter Berechtigungen wird im Besonderen verhindert, dadurch dass:

• die Zugriffsrechte (sowohl für Anwender, wie auch für Administratoren) sich an den aufgabenbedingten und datenschutzrechtlichen Erfordernissen orientieren;
• Schutz gegen unberechtigte interne und externe Zugriffe durch Verschlüsselung und Firewalls bestehen (siehe 2.).

4. Dafür Sorge zu tragen, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können, und dass es überprüft und festgestellt werden kann, an welche Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist **(Weitergabekontrolle)**:

Die Aspekte der Weitergabe personenbezogener Daten wird hierdurch umgesetzt, dass:

• VPN-Technologie (SSL/TLS) zur Datenkommunikation eingesetzt wird;
• E-Mail-Nachrichten bzw. sonstige Informationen grundsätzlich verschlüsselt bzw. anonymisiert versendet werden können;
• beim physischen Transport, geeignete Transportpersonen sorgfältig ausgewählt werden.

5. Dafür Sorge zu tragen, dass nachträglich geprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind **(Eingabekontrolle)**:

Die Kontrolle von Eingaben, erfolgt durch:

• Protokollierung und Nachvollziehbarkeit von Eingaben, Änderungen und Löschung von Daten (durch Logfiles);

• die Zugriffsrechte orientieren sich (sowohl für Anwender als auch für Administratoren) an den aufgabenbedingten und datenschutzrechtlichen Erfordernissen.

6. Dafür Sorge zu tragen, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können **(Auftragskontrolle)**:

Die Vergabe und die Überwachung von Auftragsdatenverarbeitungen insbesondere der externen Rechenzentren ergeben sich aus dem Folgenden:

• sorgfältige Auswahl von Dritten (insb. wegen Datensicherheit)
• detaillierte Regelungen zum Auftragsverhältnis;
• Vereinbarung wirksamer Kontroll- und oder Zugriffs- bzw. Löschungsrechte (ggf. Vertragsstrafen);

7. Dafür Sorge zu tragen, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind **(Verfügbarkeitskontrolle)**:

Zur Durchsetzung der Verfügbarkeit, hat das Subunternehmen veranlasst, dass:

• eine unterbrechungsfreie Stromversorgung besteht (USV);
• Räumlichkeiten in Brandabschnitten versehen mit einzelnen Brandschutzeinrichtungen (Feuer- und Rauchmeldeanlagen; Feuerlöscher) eingeteilt sind;
• Klimaanlagen vorhanden sind;

Im Rahmen des Rechenzentrumsbetriebes wird insbesondere darauf geachtet, dass:

• die Stromversorgung durch Redundanzen sichergestellt wird (Notstromaggregate sowie USV- Anlagen mit n+1 Redundanz; Überbrückungszeit mindestens 15 min. bis die Notstromaggregate die Stromversorgung wieder sicherstellen - Anlaufzeit inkl. Lastübernahme 1-2 min.);
• das Rechenzentrum mit einer Raumklimatisierung ausgestattet ist (mittlere Temperatur 24° C +/- 4°, redundant ausgelegt (n+1), entsprechende Luftfilter installiert sind;
• das Rechenzentrum über baulich getrennte Brandabschnitte verfügt. In den Räumlichkeiten ist eine Brandmeldeanlage, eine Brandfrühersterkennung sowie eine Rauchmelde- und Gaslöschanlage installiert;
• die Hochwasser- und Erdbebenkritikalität sorgfältig geprüft wurde.

8. Dafür Sorge zu tragen, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können **(Trennungskontrolle)**:

Die getrennte Datenverarbeitung wird gewährleistet durch:

• fehlende Möglichkeit eines physikalischen Zugriffs durch dedizierten Rechte und Pflichten;
• klare Trennung und Nachvollziehbarkeit von Kundenzugriffen (logische Trennung durch individuellen Benutzungsprofil mit Passwortschutz);
• getrennte Verarbeitung zweckgebundener Daten.

9. Die innerbetriebliche Organisation den besonderen Anforderungen des Datenschutzes anzupassen.

Das Subunternehmen hat sich den folgenden datenschutzrechtlichen Standards unterworfen:

• Fertigung von internen Datenschutz- und Arbeitsanweisungen;
• Regelmäßige Hinweise und Ermahnungen, um das Problembewusstsein zu fördern;
• Gelegentliche unvermutete Kontrolle der Einhaltung von Datenschutz- und Datensicherungsmaßnahmen.
• Die Leistungserbringung in einem deutschen Rechenzentrum und unter Beachtung des deutschen Datenschutzrechts erfolgt.